УДК 343.85 (477)

Марина Олександрівна КРАВЦОВА,
кандидат юридичних наук, старший викладач кафедри кримінального права і кримінології
(Харківський національний університет внутрішніх справ, Харків, Україна)

СУЧАСНИЙ СТАН І НАПРЯМИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Проаналізовано основні кількісні та якісні показники кіберзлочинності (рівень, географія, структура, динаміка). Сформульовано основні напрями протидії кіберзлочинності в Україні на загальносоціальному, спеціально-кримінологічному та індивідуальному рівнях.

Ключові слова: *кіберзлочини, кіберзлочинність, протидія кіберзлочинності, стан кіберзлочинності, динаміка кіберлочинності*

Постановка проблеми. Розповсюдження комп'ютерних технологій і комп'ютерної техніки, повсюдне проникнення телекомунікаційних мереж майже в усі сфери життєдіяльності людини одночасно і полегшило (створення та накопичення баз даних, автоматична обробка інформації, можливість миттєвого передання інформації на дуже великі відстані тощо), й ускладнило управління, виконання виробничих процесів та особисту комунікацію. Йдеться про необхідність створення безпечних умов використання віртуального простору, серед іншого захисту від небезпек, які виникають із боку злочинців. Розширення сфери використання комп'ютерних технологій, яке набуває подальшого розвитку, надає нові можливості вчинення традиційних злочинів і створює умови для реалізації принципово нових схем і методів злочинної діяльності. Актуальність протидії використанню у злочинній діяльності комп'ютерних технологій на цьому етапі розвитку української держави не викликає сумнівів. Більш того, розмах комп'ютеризації та рівень можливостей, які при цьому одержують зловмисники, й тенденція збільшення кількості злочинів у сфері

комп'ютерних інформаційних технологій становлять загрозу демократичним перетворенням в Україні та її національній безпеці.

Аналіз останніх досліджень і публікацій. Результати дослідження спеціальної літератури свідчать, що на цей момент існує досить велика кількість робіт, в яких розглядаються окремі аспекти боротьби з кіберзлочинністю. Зокрема, цій проблематиці присвячено роботи Д. С. Азарова, Ю. М. Батуріна, П. Д. Біленчука, В. М. Бутузова, В. Б. Вєхова, В. О. Голубєва, О. Ю. Іванченко, М. В. Карчевського, Н. В. Коваленко, А. А. Музики, С. О. Орлова, Д. В. Пашнєва, В. С. Цимбалюка, В. П. Шеломенцева та ін. Разом із цим швидкий розвиток комп'ютерних технологій і сфер застосування комп'ютерної техніки й динаміка поширення кіберзлочинів підтверджують, що одними з перших їх «споживачів» є злочинці. Найновітніший арсенал технічних засобів та інформація, на жаль, дуже швидко потрапляють до представників злочинного світу, адже вони не обмежені у витратах коштів та матеріальному забезпеченні, як правоохоронні органи, наприклад Департамент кіберполіції. До того ж процес виявлення та фіксації кіберзлочинів і їх наслідків ускладнюється їх латентністю та потребує постійного вдосконалення засобів протидії такому виду злочинності.

Метою статті є дослідження сучасного стану (рівень, географія, структура) та динаміки злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку, тобто кіберзлочинів в Україні, визначення напрямів протидії кіберзлочинності.

Виклад основного матеріалу. Перш ніж перейти до розгляду питань опису статистичних показників та характеристики кіберзлочинності доцільно зазначити, що з приводу визначення поняття й ознак кіберзлочинів і кіберзлочинності в науці кримінального права та кримінології досі триває дискусія, адже на національному рівні це поняття не має нормативного врегулювання (на рівні законодавчого його визначення), проте цим терміном оперує Конвенція про кіберзлочинність (2001 р.) [6].

Стосовно наукових підходів до визначення понять «кіберзлочин» і «кіберзлочинність» слід пояснити, що частина вчених пов'язує їх із специфічним предметом злочину – комп'ютером (комп'ютерною технікою) чи комп'ютерними даними та способом вчинення злочину – з використанням вищевказаних предметів для вчинення злочину [10, с. 338; 2, с. 36] або з певним місцем його вчинення, яким є кіберпростір [1, с. 17], віртуальний простір [4, с. 173].

Такі підходи, на наш погляд, є дещо спрощеними, адже, якщо визнати комп'ютер предметом злочину, то будь-яке його використання, наприклад для нанесення тілесних ушкоджень, утворюватиме склад кіберзлочину. Що стосується зв'язку кіберзлочинів та кіберзлочинності лише з певним простором (сферою) вчинення злочину (злочинів), слід звернутися до дослідження, проведеного О. В. Манжаєм. Проаналізувавши існуючі визначення кіберпростору, науковець дійшов висновку, що кіберпростір ідентифікується з певним єдиним простором – це інформаційне середовище

(простір), яке виникає (існує) за допомогою технічних (комп'ютерних) систем під час взаємодії людей між собою, взаємодії технічних (комп'ютерних) систем та управління людьми цими технічними (комп'ютерними) системами [9, с. 216], що фактично не охоплює локальні мережі (не приєднані до Інтернет), не кажучи вже про локальні комп'ютери.

Важко погодитися із можливістю назвати середовище, створене функціонуванням одного такого комп'ютера, таким об'ємним терміном, як «кіберпростір». Так само важко й навіть неможливо опиратися тому, що такий комп'ютер є комп'ютерною системою, яка згадується під час визначення кіберзлочинності й може бути використана для вчинення злочину. Таким чином, визначення кіберзлочинності через поняття кіберпростору не є достатнім для позначення її обсягу.

На наш погляд, кримінально-правовий обсяг поняття «кіберзлочинність» складають злочини, передбачені статтями 361, 361-1, 361-2, 362, 363, 363-1 КК України, що містяться у Розділі XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Під кіберзлочинністю слід розуміти соціально-правовий феномен, що проявляється в забороненій законом про кримінальну відповідальність предметній діяльності (кримінальній активності) частини населення з використанням електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку [7, с. 19]. Зазначений підхід до визначення кіберзлочинності був сприйнятий і МВС України під час установлення кола злочинів, які належать до компетенції колишнього Управління боротьби кіберзлочинності (наразі Департаменту кіберполіції Національної поліції України).

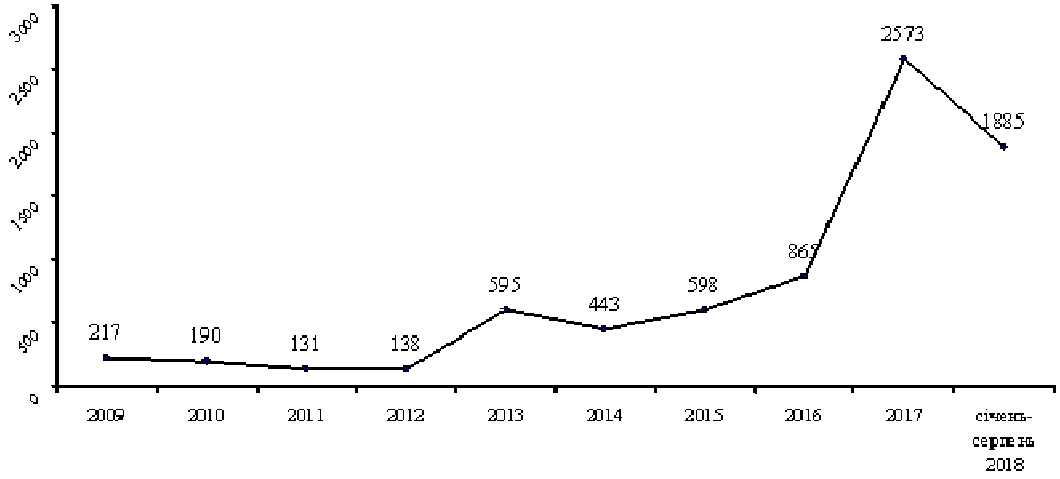
Таким чином, це дослідження ґрунтуватиметься на емпіричних даних (офіційні статистичні дані МВС та Генеральної прокуратури України), які стосуються основної, системоутворюючої групи кіберзлочинів – злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, оскільки саме специфічні властивості цих злочинів найбільш повно характеризують кіберзлочинність, а отже результати цього дослідження можна вважати репрезентативними стосовно всього масиву кіберзлочинності.

Визначаючи сучасний стан кіберзлочинності в Україні, слід указати, що вона, як і будь-яке інше соціальне явище, піддається оцінюванню за допомогою певних критеріїв, що відбивають її кількісні та якісні характеристики. Здійснити таке оцінювання можна через аналіз показників поширеності кіберзлочинності в Україні: її рівня, географії, структури, динаміки тощо.

Стосовно рівня кіберзлочинності та її динаміки зазначимо, що у 2009 р. в України було зареєстровано 217 злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, у 2010 р. – 190, у 2011 р. – 131, у 2012 р. – 138, у 2013 р. – 595, у 2014 р. – 443, у 2015 р. – 598, у 2016 р. – 865, у 2017 р. – 2573, за січень-серпень 2018 р. – 1885 злочинів *(Діаграма 1).*

Діаграма 1

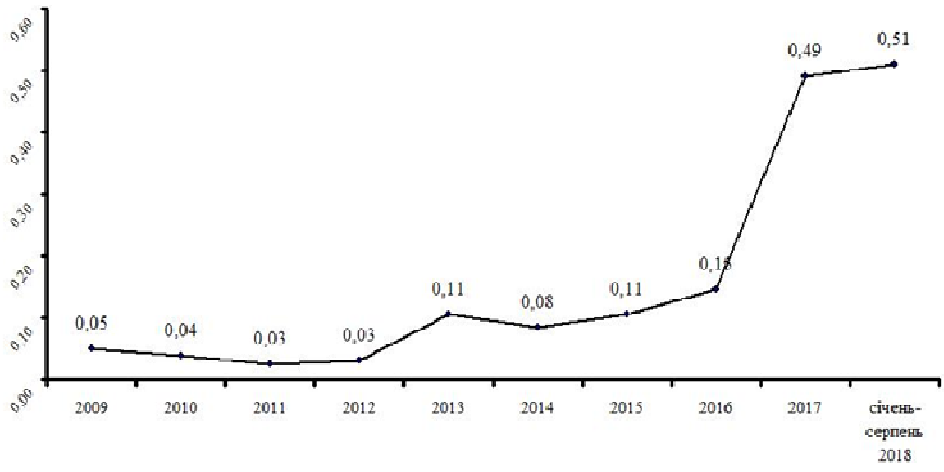
Графічне зображення рівня та динаміки кіберзлочинності в Україні за 2009 – серпень 2018 рр.



Питома вага кіберзлочинів у загальній кількості зареєстрованих злочинів становить 0,05 % від загальної кількості зареєстрованих злочинів у 2009 р., 0,04 % – у 2010, 0,03 % – у 2011, 0,03 % – у 2012, 0,11 % – у 2013, 0,08 % – у 2014, 0,11 % у – 2015, 0,15 % – у 2016, 0,49 % – у 2017 р. та 0,51 % від злочинів, зареєстрованих за січень-серпень 2018 р. (*Діаграма 2*).

Діаграма 2

Графічне зображення питомої ваги кіберзлочинів у загальній кількості зареєстрованих в Україні злочинів за 2009 – серпень 2018 рр.



Суттєве збільшення кількості зареєстрованих у 2013 р. кіберзлочинів окремі вчені пов'язують із тим, що «зростання вказаного виду злочинності обумовлено щорічним зростанням користувачів Інтернет-ресурсу в Україні» [5, с. 124], інші пов'язують різницю в даних, що стосуються обліку зареєстрованих злочинів, з переданням права формувати державну статистику про стан злочинності в державі від МВС до прокуратури України [3].

На наш погляд, з набуттям чинності Кримінальним процесуальним кодексом України (2012 р.), яким було внесено істотні зміни у порядок розслідування проваджень і компетенцію уповноважених для цього осіб, і низки супутніх документів дійсно відбулися певні коливання у статистичній картині, разом із цим їх не варто розглядати як дещо надзвичайне чи критичне. Для розуміння природного перебігу речей та відсутності істотного коливання достатньо звернути увагу на питому вагу кіберзлочинів у загальній кількості зареєстрованих злочинів, що у 2013 р. відповідала 0,11 %. Аналогічні показники ми бачимо також у 2015 р., і навпаки, у 2014 р. відбулося зниження кількості зареєстрованих кіберзлочинів.

Разом із цим особливо відчутне зростання рівня кіберзлочинності відбулося у 2017 р. (більш ніж у чотири рази порівняно з 2013 р.), і це свідчить про наявність специфічних рис досліджуваного виду злочинів, пов'язаних з особливостями комплексу факторів його детермінації, як-то: стрімке розгортання процесу інформатизації суспільства (упровадження мережі третього покоління (3G) операторами мобільного зв'язку), освоювання кібертехнологій як засобу злочинної діяльності, об'єктивне відставання технічної складової правоохоронної системи (активна фаза реформування органів Національної поліції України, відсутність достатньої кількості фахівців та недостатнє фінансування) тощо.

Статистичний аналіз географічної поширеності кіберзлочинів в Україні за останні роки виявив залежність від фактору урбанізації. Найвища кіберкримінальна активність фіксується за ранжиром у Дніпропетровській області, м. Києві, а також у Харківській, Запорізькій та Черкаській областях; найнижча – в Чернівецькій, Херсонській, Сумській і Кіровоградській.

Відповідні географічні особливості вчинення кіберзлочинів в Україні слід розглядати не стільки через призму переважання на мапі кіберзлочинів східних областей порівняно із західними (що традиційно пояснюється низкою чинників, як-то: густота населення, яка на Сході нашої держави є вищою ніж на Заході, історичні та культурологічні передумови тощо), скільки через призму переважання промислово та фінансово розвинутих областей (центрів). Саме технічний (відповідно, й фінансовий) розвиток є неможливим без залучення сучасних, перш за все інформаційних технологій, середовище яких і є середовищем кіберзлочинності.

При цьому аналіз «географічних» особливостей окремих видів кіберзлочинів дозволив виявити таку специфіку. Деякі злочини мають традиційну «приналежність» за місцем вчинення переважно до великих міст. Це такі злочини, як створення з метою використання, розповсюдження або збуту шкідливих програм чи технічних засобів, а також їх

розповсюдження або збут; несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації та порушення правил експлуатації автоматизованих ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється. Такий злочин, як несанкціоноване втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, маючи спочатку переважно приналежність до великих міст, останнім часом дедалі більше (в середньому 50 %) учиняється у містах та селищах міського типу.

Що стосується несанкціонованих дії з інформацією, яка обробляється в ЕОМ (комп'ютерах), автоматизованих системах і комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, то цей злочин порівняно з іншими кіберзлочинами має найбільш виражену тенденцію стрімкої «переорієнтації» на невеликі міста та сільську місцевість.

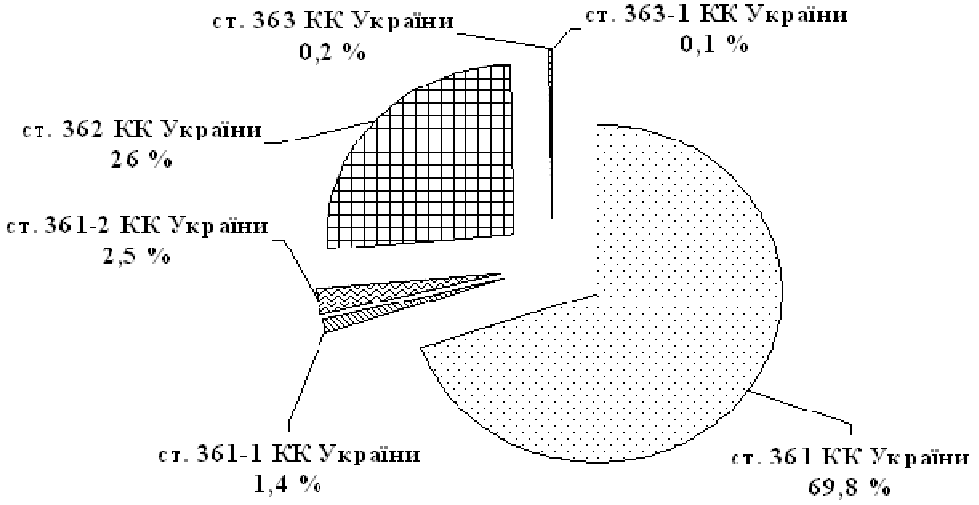
Статистичні дані, що характеризують показники злочинності в Україні за 2017 р., дозволяють зробити висновок, що кіберзлочинність становить 0,49 % (при цьому злочини проти волі, честі та гідності особи складають 0,18 %, а злочини проти статевої свободи та статевої недоторканості особи – 0,16 %) від загальної кількості злочинів, облікованих у звітному періоді.

Аналіз даних офіційної статистичної звітності за 2017 р. показав, що переважну більшість у структурі досліджуваних кіберзлочинів, зокрема злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, становлять ті, відповідальність за які передбачено ст. 361 КК України – несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (69,8 %). На другому місці – злочин, передбачений ст. 362 КК України, – несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (26 %). На третьому місці – злочин, передбачений ст. 361-2 КК України, – несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (2,5 %). На четвертому – злочин, передбачений ст. 361-1 КК України, – створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (1,4 %). Усі інші злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку складають 0,3 %. Співвідношення кіберзлочинів у межах групи злочинів у сфері використання електронно-

обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку можна відобразити у вигляді діаграми *(Діаграма 3)*.

Діаграма 3

Структура злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж



У структурі кіберзлочинності в Україні переважає несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України). На нього припадає понад 69,8 % злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, які вчиняються (реєструються) на території України.

Незважаючи на мінливу динаміку, рівень кіберзлочинності в абсолютних показниках характеризується істотним зростанням і стабілізацією показників на високих позначках, а дослідження співвідношення частки їх складових у динаміці вказує на негативні тенденції змін кількісно-якісних характеристик цього виду злочинів і дозволяє виявити, за рахунок яких злочинів головним чином відбувається приріст *(Таблиця 1).*

Таблиця 1

Кримінально-правова структура кіберзлочинності в Україні у динаміці за 2013–2017 рр.

Обліковано кримінальних правопорушень у звітному періоді	**2013**	**2014**	**2015**	**2016**	**2017**
Несанкціоноване втручання в роботу електронно-обчислювальних машин	408	344	432	494	1795

(комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України)					
Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1 КК України)	12	10	21	15	35
Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2 КК України)	20	11	59	28	64
Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК України)	152	73	75	311	670
Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України)	2	4	9	15	6
Перешкоджання роботі електронно-обчислювальних	1	1	2	2	3

машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1 КК України)					
Разом	595	443	598	865	2573

Кіберзлочинність – за своєю природою транскордонне явище, що дозволяє більшості вчених вказувати на те, що для кіберзлочинів є характерним максимальний рівень латентності. Факторами латентності кіберзлочинів виступають такі: 1) складність механізму вчинення кіберзлочинів, поєднана з дуже різноманітними сферою та наслідками їх учинення, а також «комп'ютерна безграмотність» більшості потенційних жертв кіберзлочинів, їх нехтування своєю безпекою; 2) негативна поведінка жертв (очевидців) злочину – незвернення жертви та осіб, яким відомо про злочин, до правоохоронних органів і неповідомлення про факт вчинення кіберзлочину; 3) недоліки в роботі правоохоронних органів стосовно реагування на звернення та повідомлення про кіберзлочини.

Розглядаючи питання протидії кіберзлочинності, доцільно приєднатися до тих науковців-кримінологів, які виокремлюють загальносоціальні, спеціально-кримінологічні й індивідуальні напрями протидії.

Протидія кіберзлочинності на загальносоціальному рівні (напрямі) передбачає комплекс перспективних соціально-економічних, організаційно-управлінських, ідеологічних, культурно-виховних та інших заходів, спрямованих на вирішення нагальних соціальних проблем і суперечностей у країні. Саме реалізація загальносоціальних заходів запобігання дає змогу усунути чи мінімізувати вплив криміногенних факторів детермінації кіберзлочинності, запобігти формуванню особистості злочинця.

Задля належної розробки відповідних заходів протидії злочинності, в тому числі кіберзлочинності, є необхідною належна організація діяльності як правоохоронних органів, так і вищих органів держави, яка відповідає вимогам, що висуваються до правової, незалежної та демократичної держави. Крім того, необхідно усувати фактори, що позитивно впливають на існування та розвиток злочинності [8].

Спеціально-кримінологічне запобігання стосується безпосередньо діяльності Національної поліції України і спрямовується головним чином на окремі соціальні групи, які привертають увагу суб'єктів превентивної діяльності.

Основними заходами запобігання кіберзлочинності, що повинні реалізовувати ОВС та Національною поліцією (в особі Департаменту кіберполіції), слід визнати такі: розроблення та затвердження МВС Стратегії протидії кіберзлочинності, що повинна містити концепцію кримінально-

превентивої діяльності, науково обґрунтовані стратегічні й тактичні заходи антикримінального впливу й моніторингові механізми забезпечення якості останнього; збільшення кількості планових і позапланових перевірок відповідними органами поліції підприємств, установ та організацій, діяльність яких прямо пов'язана з використанням комп'ютерних технологій або наданням інформаційних послуг, з метою виявлення випадків використання нелегального (нерегламентованого) програмного забезпечення; посилення відповідальності уповноважених осіб підприємств, установ або організацій, діяльність яких пов'язана із зазначеною сферою, які за своїми посадовими або функціональними обов'язками відповідають за безпеку функціонування комп'ютерів та комп'ютерних мереж; установлення жорсткого контролю за обігом будь-яких технічних засобів, заборонених для використання у вільному обігу або використання яких є обмеженим (технічні засоби для негласного зняття інформації з каналів зв'язку, прослуховування, перехоплення кодованих сигналів, добору паролів тощо); використання позитивного досвіду діяльності правоохоронних органів інших країн у цій сфері (в першу чергу аналізуються стан технічного забезпечення й технології, що використовуються для запобігання вчиненню зазначених злочинів); участь працівників «кіберполіції» у міжнародних семінарах, круглих столах тощо, присвячених указаній проблематиці, та ініціювання відповідними органами нашої держави проведення таких заходів на території України.

Напрямом діяльності щодо протидії вчиненню кіберзлочинів слід також визначити виявлення осіб, які вчиняють або схильні до вчинення кіберзлочинів, індикаторами поведінки яких є систематичний перезапис даних без необхідності, заміна або видалення даних, поява фальшивих записів, випадків, коли оператор системи без об'єктивних підстав починає працювати наднормово, персонал заперечує проти здійснення контролю за записом даних, фіксуються постійні скарги користувачів баз даних або власників щодо помилок та затримок у роботі системи тощо.

Окремим заходом запобігання вчиненню кіберзлочинів є виявлення та запобігання діяльності кібертерористів, тобто осіб, які використовують комп'ютерну техніку, пристрої та мережі для вчинення терористичних актів [11, с. 408].

Висновки та перспективи подальших досліджень. Рівень кіберзлочинності у 2017 р. склав 2573 злочинів і має тенденцію до зростання. Показники динаміки кіберзлочинності в цілому відповідають показникам загальної злочинності в країні, що свідчить про специфічність детермінаційного комплексу кіберзлочинності та про відставання можливостей правоохоронних органів від сучасного рівня технологічного та програмного забезпечення кримінальної активності. Найбільш ефективними заходами, безпосередньо спрямованими на протидію кіберзлочинності, є такі: збільшення кількості планових і позапланових перевірок; установлення жорсткого контролю за обігом технічних засобів, заборонених або обмежених у вільному цивільному обігу; перейняття

досвіду діяльності правоохоронних органів інших країн у цій сфері; співробітництво з відповідними органами інших країн щодо розкриття, розслідування та запобігання злочинам в аналізованій сфері, обмін досвідом правозастосування; виявлення осіб, схильних до вчинення злочинів в аналізованій сфері, тощо. Указані заходи потребують подальших наукових розробок для створення дієвих інструментів протидії сучасним викликам кіберзлочинності.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Бутузов В. М. Співвідношення понять «комп'ютерна злочинність» та «кіберзлочинність». *Інформаційна безпека людини, суспільства, держави*. 2010. № 1 (3). С. 16–18.

2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия. Москва : Право и закон, 1996. 182 с.

3. Петер Геннадій. Прокуратура та правоохоронні органи України в період злочинного режиму Януковича і її перетворення сьогодні. URL: http://www.3republic.org.ua/ua/ideas/13397 (дата звернення: 14.09.2018).

4. Іванченко О. Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. *Актуальні проблеми вітчизняної юриспруденції.* 2016. Вип. 3. С. 172–177.

5. Книженко О. О. Сучасний стан злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку в Україні. *Бюлетень Міністерства юстиції України*. 2014. № 7. С. 122–127.

6. Конвенція про кіберзлочинність : міжнародний документ від 23.11.2001 // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 10.09.2018).

7. Кравцова М. О., Литвинов О. М. Запобігання кіберзлочинності в Україні : монографія. Харків : Панов, 2016. 212 с.

8. Кравцова М. О. Фактори детермінації кіберзлочинності в сучасній кримінологічній теорії. *Юридичний науковий електронний журнал*. 2014. № 5. С. 110–113. URL: http://lsej.org.ua/5_2014/5_2014.pdf (дата звернення: 10.09.2018).

9. Манжай О. В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і Безпека*. 2009. № 4. С. 215–219.

10. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби // Теоретичні та прикладні питання економіки : зб. наук. пр. Київ : Вид.-поліграф. центр «Київ. ун-т», 2009. Вип. 19. С. 338–342.

11. Кримінологія. Академічний курс / кол. авт. ; за заг. ред. О. М. Литвинова. Київ : Кондор, 2018. 588 с.

Стаття надійшла до редакції 15.09.2018.

Марина Александровна КРАВЦОВА,
кандидат юридических наук, старший преподаватель
(Харьковский национальный университет внутренних дел, Харьков, Украина)

СОВРЕМЕННОЕ СОСТОЯНИЕ И НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В УКРАИНЕ

Проанализированы основные количественные и качественные показатели киберпреступности (уровень, география, структура, динамика). Сформулированы основные направления противодействия киберпреступности в Украине на общесоциальном, специально-криминологическом и индивидуальном уровнях.

Ключевые слова: *киберпреступления, киберпреступность ,состояние киберпреступности, динамика киберпреступности, противодействие киберпреступности.*

Maryna O. KRAVTSOVA
candidate of law sciences, Senior lecturer
(Kharkiv National University of Internal Affairs, Kharkiv, Ukraine)

MODERN STATUS AND DIRECTIONS OF COUNTERACTION OF CYBERCRIME IN UKRAINE

The author of the article has analyzed the main quantitative and qualitative indicators of cybercrime (the level, geography, structure, dynamics). The author has formulated the basic directions for counteracting cybercrime in Ukraine at national, special criminological and individual levels.

Key words: *computer-related crimes, cybercrime, the state of cybercrime, the dynamics of cybercrime, counteraction to cybercrime.*